UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

DENNIS CASTILLE, on behalf of himself and all others similarly situated, Plaintiff, v. **VERISOURCE SERVICES, INC.**, Defendant.	Case No. **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Dennis Castille ("Plaintiff"), individually and on behalf of all similarly situated persons (the "Class" or "Class Members"), alleges the following against VeriSource Services, Inc. ("VSI" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against VSI for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as its regular business practices, including Plaintiff's and Class Members' full names and Social Security numbers (collectively "PII" or "Private Information").

2. VSI, headquartered in Houston, Texas, is a company that specializes in providing employee benefits administration and enrollment solutions.

3. Upon information and belief, current and former employees of Defendant's clients are required to entrust Defendant with sensitive, non-public PII, without Defendant could not perform its regular business activities, in order to obtain employment or certain employment benefits at Defedant's clients.

4. On or about May 4, 2024, VSI filed an official incident notice of a hacking incident with the Office of the Attorney General in Maine.

5. Between August 20, 2024, and August 21, 2024, VSI filed additional incident notices with the Offices of the Attorney General in California and Texas.

6. On or about August 20, 2024, VSI also sent out data breach letters ("Notice Letter") to individuals whose information was compromised as a result of the hacking incident.

7. Based on the Notice Letter, on February 28, 2024, VSI discovered "unusual activity that disrupted access to certain systems."[1] In response, the company launched an investigation, confirming that an unauthorized party had accessed certain PII stored in its system on or about February 27, 2024 (the "Data Breach").

8. Plaintiff and Class Members were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

9. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, full names and Social Security numbers that VSI collected and maintained.

[1] *See* Notice Letter https://oag.ca.gov/ecrime/databreach/reports/sb24-590489 (last visited October 8, 2024).

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. There has been no assurance offered by VSI that all personal data or copies of data have been recovered or destroyed, or that VSI has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

12. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

13. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to VSI, and thus, VSI was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, VSI and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information. Had VSI properly monitored its networks effectively, it would have discovered the Data Breach sooner.

15. The Plaintiff's and Class Members' identities are now at risk because of VSI's negligent conduct, as the Private Information that VSI collected and maintained is now in the hands of data thieves and other unauthorized third parties.

16. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

17. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

18. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) uncompensated lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and

abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

19. Plaintiff brings this class action lawsuit to address VSI's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

20. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

21. Dennis Castille is, and at all times mentioned herein was, an individual citizen of the state of Louisiana.

22. Defendant VeriSource Services, Inc. is a company that specializes in providing employee benefits administration and enrollment solutions 7600 W Tidwell Road, Suite 700, Houston, Texas.

III. JURISDICTION AND VENUE

23. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, and at least one member of the class is a citizen of a state different from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. This Court has personal jurisdiction over Defendant because its principal place of business is located in the Houston Division of the Southern District of Texas, regularly conducts

business in Texas, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District. The Defendant is a citizen of Texas.

Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District.

IV. FACTUAL ALLEGATIONS

Background of Defendant

25. Founded in 1997, VSI is a company that provides "employee benefit administrative and enrollment solutions to employee-benefit management companies groups[.]"[2]

26. Plaintiff and Class Members are current and former employees of Defendant's clients.

27. In order to apply to be an employee or obtain certain employment-related benefits at Defendant's clients, Plaintiff and Class Members were required to provide Defendant with their sensitive and confidential PII, including their names and Social Security numbers.

28. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

29. Upon information and belief, Defendant made promises and representations to its clients' employees, including Plaintiff and Class Members, that the PII collected from them as a condition of their employment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

[2] *See* http://www.verisource.com/Home/About/2 (last visited Oct. 8, 2024).

30. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

32. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information.

33. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

34. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its clients' employees' PII safe and confidential.

35. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

36. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

38. Plaintiff and Class Members relied on VSI to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

The Data Breach.

39. On or about August 20, 2024, Defendant began sending Plaintiff and other victims of the Notice Letter, informing them that:

> **What Happened?** On February 28, 2024, VSI became aware of unusual activity that disrupted access to certain systems. Upon discovery, VSI immediately took steps to secure its network and engaged a leading, independent digital forensics and incident response firm to investigate what happened and whether any sensitive data may have been impacted. The investigation subsequently revealed certain personal information was acquired without authorization by an unknown actor on or about February 27, 2024. VSI undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, which concluded on April 23, 2024. We then took steps to notify you of the incident as quickly as possible. Please note that VSI has no evidence of any actual or suspected misuse of information involved in this incident.
>
> **What Information Was Involved?** The information that was potentially impacted during this incident may have included your name, as well as your Social Security number.

40. Defendant failed to promptly notify affected individuals in the Data Breach. While Defendant discovered suspicious access in February 2024, it did not notify affected individuals until about August 2024, approximately six full months after the Data Breach occurred. This significant delay in notification further prevented individuals from taking timely action to protect their Private Information, potentially exacerbating the impact of the Data Breach and leaving them vulnerable to identity theft and fraud.

41. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To

date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

42. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

43. VSI also acknowledged that its data security was insufficient by discussing various additional steps they took, after the Data Breach, to "enhance our security posture and reduce the risk of similar future incidents"

44. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant's networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiff's and Class Members' Social Security numbers for download and theft.

45. In the context of notice of data breach letters of this type, Defendant's use of the phrase "potentially impacted" is misleading lawyer language. Companies only send notice letters because data breach notification laws require them to do so. And such letters are only sent to those persons who Defendant itself has a reasonable belief that such personal information was accessed

46. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members

should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

47. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

48. VSI had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

49. Plaintiff and Class Members provided their Private Information to VSI with the reasonable expectation and mutual understanding that VSI would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

50. VSI's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

51. VSI knew or should have known that its electronic records would be targeted by cybercriminals.

52. The attacker targeted, accessed, and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiff and Class Members, including their names and Social Security numbers. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

53. Plaintiff further believes that his PII and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

54. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

52. Defendant failed to implement reasonable security procedures and practices commensurate with the sensitivity of the information held for Plaintiff and Class Members. This neglect led to the exposure of their Private Information, due to insufficient measures like encryption or the proper deletion of data when no longer necessary.

53. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[3]

54. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

[3] *See How to Protect Your Networks from RANSOMWARE*, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited on Oct. 8, 2024).

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[4]

55. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

[4] *Id.* at 3-4.

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit;
- Remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[5]

[5] *See Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited on Oct. 8, 2024).

56. Given that Defendant was storing the Private Information of its clients' current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

57. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief, at least thousands to tens of thousands of individuals, including that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Its Clients' Employees' Private Information

58. Defendant acquires, collects, and stores a massive amount of Private Information of its clients' employees.

59. As a condition of obtaining employment at Defendant's clients, Defendant requires that its clients' employees and other personnel entrust it with highly sensitive personal information.

60. By obtaining, collecting, and using Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

61. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

62. Upon information and belief, in the course of collecting Private Information from its clients' employees, including Plaintiff, Defendant promised to provide confidentiality and

adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

63. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew, Or Should Have Known, of the Risk Because Employee-Benefit Companies In Possession Of Private Information Are Particularly Susceptible To Cyber Attacks

64. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting employee-benefit companies that collect and store Private Information, like Defendant, preceding the date of the breach.

65. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting employee-benefit management companies that collect and store PII and other sensitive information, like Defendant, preceding the date of the breach.

66. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[6] Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.[7] The 2023 compromises represent a

[6] *See 2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024); https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (Last visited on Oct. 8, 2024).
[7] *Id.*

78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021. [8]

67. In light of recent high-profile data breaches at other industry-leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

68. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

69. Additionally, as companies became more dependent on computer systems to run their business,[10] *e.g.*, working remotely as a result of the COVID-19 pandemic, and the Internet of

---

[8] *Id.*

[9] *See* Ben Kochman, *FBI, Secret Service Warn Of Targeted Ransomware*, Law360, https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited on Oct. 8, 2024).

[10] *See Implications of Cyber Risk for Financial Stability*, https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last visited on Oct. 8, 2024).

Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[11]

70. Defendant knew and understood unprotected or exposed Private Information in the custody of financial services companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

71. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

72. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

73. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

74. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—

[11] *See* Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last visited on Oct. 8, 2024).

particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

75. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

76. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive Private Information was, in fact, affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

77. As an employee-benefit company in the custody of the Private Information of its clients' employees, Defendant knew or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifying Information

78. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." [12]

[12] 17 C.F.R. § 248.201 (2013).

79. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

80. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

81. Numerous sources cite dark web pricing for stolen identity credentials.[14]

82. For example, Personal Information can be sold at a price ranging from $40 to $200.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

83. For example, Social Security numbers are among the worst kinds of Private Information to be stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

84. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards

---

[13] *Id.*

[14] *See Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Oct. 8, 2024).

[15] *See Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Oct. 8, 2024).

[16] *See In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited on Oct. 8, 2024).

> and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

85. What's more, it is not easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse.

86. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

87. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

88. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035

[17] *See* Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited on Oct. 8, 2024).

[18] *See* Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited on Oct. 8, 2024).

(D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target his in fraudulent schemes and identity theft attacks.")

89. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."

90. Next to a Social Security number, a driver's license number is one of the most crucial pieces of information that must be safeguarded against theft.

91. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable: "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity—which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[19]

[19] *See Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, *available at:* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited on Oct. 8, 2024).

92. A driver's license is an identity thief's paradise. Access to this single number can provide identity thieves with multiple pieces of personal information, such as an individual's birthdate, address, height, eye color, and signature. A driver's license is also linked to vehicle registration, insurance policies, and records maintained by the Department of Motor Vehicles, employers, medical offices, government agencies, and other entities. [20]

93. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[21] However, this is clearly not the case in the context of the Data Breach, where hackers stole this information. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[22]

94. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[23]

---

[20] *See What Should I Do if My Driver's License Number is Stolen?*, Experian, https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited on Oct. 8, 2024).

[21] *See Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine, *available at*: https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Oct. 8, 2024).

[22] *Id.*

[23] *See How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Oct. 8, 2024).

95. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

96. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers, dates of birth, and names.

97. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[24]

98. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

99. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used.

100. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

---

[24] *See* Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited on Oct. 8, 2024).

[25] *See Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Oct. 8, 2024).

101. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

VSI Failed to Comply with FTC Guidelines

55. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

56. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

57. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.

58. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone

is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

59. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

60. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA.

61. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. These FTC enforcement actions include actions against employee-benefit companies, like VSI.

63. As evidenced by the Data Breach, VSI failed to properly implement basic data security practices.

64. VSI's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

65. VSI was at all times fully aware of its obligation to protect the Private Information of Private Information it retained yet failed to comply with such obligations.

66. Defendant was also aware of the significant repercussions that would result from its failure to do so.

VSI Failed to Comply with Industry Standards

67. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

68. Some industry best practices that should be implemented by businesses like VSI include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

69. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

70. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

71. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

VSI Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

72. In addition to its obligations under federal and state laws, VSI owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

73. VSI owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

74. VSI breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. VSI's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect Private Information stored in its systems;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its retained Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

75. VSI negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

76. Had VSI remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

77. Accordingly, Plaintiff's and Class Members' lives were severely disrupted.

78. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

Common Injuries & Damages

79. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Data Breaches Increase Victims' Risk Of Identity Theft

52. The unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

53. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

54. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

55. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

56. Due to the risk of one's Social Security number being exposed, state legislatures have passed laws in recognition of the risk: "[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[26]

57. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[27]

58. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[28] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account"[29]

---

[26] *See* N.C. Gen. Stat. § 132-1.10(1).

[27] *See* Husayn Kassal, *BankThink Banks need to stop relying on Social Security numbers*, American Banker, https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers (last visited on Oct. 8, 2024).

[28] *See* Ann Carrns, *Just 5 Banks Prohibit Use of Social Security Numbers*, The New York Times, https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/ (last visited on Oct. 8, 2024).

[29] *See What Can Someone Do with Your Social Security Number*, https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (last visited on Oct. 8, 2024).

59. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[30]

60. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

61. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers.

62. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

[30] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz is usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited on Oct. 8, 2024).

63. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiff and the other Class Members.

64. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

65. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

66. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

67. Thus, due to the actual and imminent risk of identity theft, VSI, in its Notice Letter includes a two-page instruction of recommended steps for Plaintiff and Class Members to take. [31]

68. VSI recommends Plaintiff and Class members to "remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company

[31] *See* Notice Letter, https://oag.ca.gov/ecrime/databreach/reports/sb24-590489 (last visited on Oct. 8, 2024).

with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC)."[32]

69. In addition, Defendant recommends that Plaintiff and Class Members to partake in activities such as placing security freezes on their accounts, placing fraud alerts on their accounts, and contacting consumer reporting bureaus.[33]

70. Defendant's extensive suggestion of steps that Plaintiff and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiff and Class Members must undertake in response to the Data Breach. Plaintiff's and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiff and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

102. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, monitoring financial accounts, changing passwords, contacting financial institutions, signing up for credit monitoring service, monitoring identity theft, reviewing credit reports, and blocking unsolicited spam communications.

71. Accordingly, the Data Breach has caused Plaintiff and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

---

[32] *Id.*
[33] *Id.*

72. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

73. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

74. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[36]

Future Costs of Credit and Identity Theft Monitoring is Reasonable and Necessary.

[34] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited on Oct. 8, 2024).

[35] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited on Oct. 8, 2024).

[36] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited on Oct. 8, 2024).

75. Given the nature of the targeted attack, the sophistication of the criminal activity, and the type of PII involved, there is a strong likelihood that entire batches of stolen information have been, or will be, placed on the black market or dark web for sale to criminals intending to use the PII for identity theft crimes. This could include activities such as opening bank accounts in victims' names to make purchases or launder money, filing false tax returns, taking out loans or lines of credit, or submitting false unemployment claims.

76. Such fraud may go undetected until debt collection calls begin, which could occur months or even years later. An individual may not realize that their PII was used to apply for unemployment benefits until law enforcement notifies the individual's employee-benefit management companies of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's legitimate tax return is rejected.

77. Consequently, Plaintiff and Class Members face an increased risk of fraud and identity theft for many years into the future.

78. The retail cost of credit monitoring and identity theft protection can be approximately $200 per year for each Class Member. This is a reasonable and necessary expense to monitor and protect Class Members from the risks of identity theft stemming from Defendant's Data Breach.

Plaintiff Dennis Castille's Experience

80. Upon information and belief, Defendant obtained Plaintiff's PII in the course of its regular business operations.

81. Upon Plaintiff Castille's employment, he was required to provide substantial amounts of his Private Information to his employer, Frank's International N.V. ("Frank's"), a client of Defendant VSI.

82. Plaintiff Castille was an employee of Frank's from 1968 until his retirement in 2015. As a retiree, his PII should no longer be necessary to be retained in VSI's system.

83. However, at the time of the Data Breach—on or about February 27, 2024—Defendant still retained Plaintiff's PII in its system, which is about nine (9) years after Plaintiff Castille's retirement.

84. On or about August 20, 2024, Plaintiff Castille received a letter entitled "Notice of Data Security Incident" which informed him that his Private Information had been inappropriately viewed and obtained during the Data Breach.

85. The Notice Letter informed him that the Private Information compromised during the Data Breach included his name and Social Security number.

86. The Notice Letter offered Plaintiff Castille only 12 months of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Castille will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

87. Plaintiff Castille is very careful about sharing his sensitive PII. He securely stores all documents containing his PII in a safe location and has never knowingly transmitted unencrypted sensitive PII over the internet or through any unsecured channels.

88. Plaintiff Castille would not have provided his private information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to protect sensitive information from theft and that those systems were subject to a data breach.

89. Plaintiff Castille suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach. Moreover, Plaintiff Castille was forced to freeze his credit as a result of the Data Breach.

90. As a result of the Data Breach, Plaintiff Castille has encountered a significant increase in suspicious and unsolicited communications, including both spam texts and calls.

91. Plaintiff Castille made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the breach, reviewing financial accounts for signs of identity theft or fraudulent activity, freezing his credit, blocking unsolicited communications, and researching the credit monitoring services offered by Defendant, as well as monitoring fraud alerts and potential dark web activity.

92. Plaintiff Castille suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

93. Since becoming aware of the Data Breach, Plaintiff Castille has already spent at least ten (10) hours addressing its impact—time that would have otherwise been spent on other important activities. This misuse of his PII was, upon information and belief, facilitated by the ability of cybercriminals to easily utilize the information compromised in the Data Breach to gather additional details about an individual, such as their phone number or email address, from publicly available sources. These sources include websites that aggregate and associate personal information with the individuals to whom it belongs.

94. Plaintiff Castille has suffered emotional distress due to the release of his private information to cybercriminals, which he believed would be safeguarded from unauthorized access and disclosure. This distress manifests as anxiety regarding the potential for unauthorized parties to view, sell, or use his private information to commit cybercrimes and other offenses against him. Plaintiff Castille is deeply concerned about the substantial and ongoing risk of identity theft and

fraud resulting from the Data Breach, as well as the significant consequences these issues may have on his life.

95. Plaintiff Castille also suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

96. Plaintiff Castille further suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant retained; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

97. As a result of the Data Breach, Plaintiff Castille anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

98. Plaintiff Castille has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

99. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

100. As a direct and proximate result of VSI's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having credit card accounts opened in their names, and other forms of identity theft.

101. Further, as a direct and proximate result of VSI's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

102. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

103. The Private Information maintained by and stolen from Defendant' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

104. Plaintiff and Class Members also lost the benefit of the bargain they made with VSI. When agreeing to obtain employment at Defendant's clients under certain terms, Plaintiff and other reasonable employees understood and expected that Defendant would adequately safeguard and protect their PII. However, Defendant failed to provide the expected level of data security. As a result, Plaintiff and Class Members received employment positions of lesser value than what they reasonably anticipated based on the agreements made with Defendant's clients.

105. Additionally, as a direct and proximate result of VSI's conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

106. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

107. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

108. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[37] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can, in turn, receive up to $50 a year.[38]

109. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss.

110. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

111. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value

[37] *See How Data Brokers Profit from the Data We Create*, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Oct. 8, 2024).
[38] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 8, 2024).

of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

g. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

112. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of VSI, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

113. As a direct and proximate result of VSI's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

114. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

115. The Class that Plaintiff seeks to represent is defined as follows:

> All individuals in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach, including all who were sent a notice of the Data Breach on or about August 20, 2024.

116. Excluded from the Class are VSI and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned, as well as their judicial staff and immediate family members.

117. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class before the Court determines whether certification is appropriate.

118. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

119. Numerosity. The Class Members are so numerous that the joinder of all members is impracticable. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, tens of thousands of individuals were impacted. The identities of Class Members are ascertainable through VSI's records, Class Members' records, publication notice, self-identification, and other means.

120. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether VSI engaged in the conduct alleged herein;

b. When VSI learned of the Data Breach;

c. Whether VSI's response to the Data Breach was adequate;

d. Whether VSI unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether VSI failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether VSI's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether VSI's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether VSI owed a duty to Class Members to safeguard their Private Information;

i. Whether VSI breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether VSI had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether VSI breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether VSI knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of VSI's misconduct;

o. Whether VSI's conduct was negligent;

p. Whether VSI's conduct was *per se* negligent;

q. Whether VSI breached third-party beneficiary contract;

r. Whether VSI was unjustly enriched;

s. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

t. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

u. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

121. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

122. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

123. Predominance. VSI has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same

computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from VSI's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages for the judicial economy.

124. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would, therefore, have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for VSI. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

125. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). VSI has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate to the Class as a whole.

126. Finally, all members of the proposed Class are readily ascertainable. VSI has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by VSI.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and All Class Members)

127. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

128. VSI requires its clients' employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of business operations.

129. VSI knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

130. VSI knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. VSI was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

131. VSI owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. VSI's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect retained Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

132. VSI's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

133. Defendant' duty also arose because Defendant were bound by industry standards to protect confidential Private Information stored in its systems.

134. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and VSI owed them a duty of care to not subject them to an unreasonable risk of harm.

135. VSI, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within VSI's possession.

136. VSI, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

137. VSI, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

138. VSI breached its duties, and thus, was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to remove or delete information it no longer requires;

c. Failing to adequately monitor the security of its networks and systems;

d. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to comply with the FTCA;

139. VSI had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust VSI with their Private Information was predicated on the understanding that VSI would take adequate security precautions. Moreover, only VSI had the ability to protect its systems (and the Private Information that it stored on them) from attack.

140. VSI's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

141. VSI's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

142. As a result of VSI's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

143. VSI also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

144. As a direct and proximate result of VSI's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

145. The injury and harm that Plaintiff and Class Members suffered were reasonably foreseeable.

146. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

147. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring VSI to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiff and All Class Members)

148. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

149. Pursuant to Section 5 of the FTCA, VSI had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

150. VSI breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

151. Plaintiff and Class Members are within the class of persons that the FTCA is intended to protect.

152. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of VSI's duty in this regard.

153. VSI violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

154. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to VSI's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

155. VSI's violations of the FTCA constitute negligence *per se*.

156. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to VSI's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

157. As a direct and proximate result of VSI's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

158. VSI breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

159. As a direct and proximate result of VSI's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

160. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring VSI to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and All Class Members)

161. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

162. Defendant entered into written contracts with its clients to provide employee-benefit management and administration services.

163. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered

into between Defendant and its clients. Defendant knew that, if it were to breach these contracts with its clients, its clients' employees—Plaintiff and Class Members—would be harmed.

164. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

165. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

166. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

167. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and All Class Members)

168. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

169. This Count is pleaded in the alternative to Counts III and IV above.

170. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their PII to Defendant. In exchange, Plaintiff and Class Members should have had their PII protected with adequate data security.

171. VSI knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

172. VSI failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

173. VSI knew that Plaintiff and Class Members conferred a benefit upon it, which VSI accepted.

174. If Plaintiff and Class Members had known that Defendant had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

175. Due to VSI's conduct alleged herein, it would be unjust and inequitable under the circumstances for VSI to be permitted to retain the benefit of its wrongful conduct.

176. As a direct and proximate result of VSI's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in VSI's possession and is subject to further unauthorized disclosures so long as VSI fails to undertake appropriate and

adequate measures to protect Private Information in its continued possession; and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

177. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from VSI and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by VSI from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

178. Plaintiff and Class Members may not have an adequate remedy at law against VSI, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Classes described above, seeks the following relief:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting

personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect himself;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: October 9, 2024.

Respectfully submitted,

/s/ William B. Federman

William B. Federman
Tex. Bar No. 00794935
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
-and-
212 W. Spring Valley Rd.
Richardson, TX 75081
Telephone: (405) 235-1560
Fax: (214) 239-2112
wbf@federmanlaw.com

M. Anderson Berry*
Gregory Haroutunian*
Michelle Zhu*
CLAYEO C. ARNOLD,
A PROFESSIONAL CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
mzhu@justice4you.com

Attorneys for Plaintiff and the putative Class

**Pro Hac Vice forthcoming*